Компания отчиталась о росте числа атак на Customer Identity Cloud.

Компания Okta — это американская технологическая компания, специализирующаяся на обеспечении идентификации, аутентификации и управлении доступом для приложений и сервисов в облаке. Основана в 2009 году Тоддом МакЛенном и Фредом Шефелбайном. Одним из основных продуктов Okta является идентификационная платформа, которая позволяет организациям обеспечивать безопасный доступ к своим приложениям и данным.

 Компания предоставляет решения для управления идентификацией и доступом как для внутренних систем и сотрудников, так и для внешних пользователей, клиентов и партнеров. Продукты Okta также включают в себя инструменты для многофакторной аутентификации, одноразовых паролей и других технологии для обеспечения безопасности в цифровом пространстве." data-html="true" data-original-title="Okta" >Okta сообщила о росте числа атак методом подстановки учётных данных на фирменную облачную платформу идентификации клиентов Customer Identity Cloud (CIC) от Okta – это облачная платформа для управления идентификацией и доступом пользователей. Она позволяет организациям безопасно и удобно управлять доступом клиентов к их приложениям и услугам. Основные функции CIC включают многофакторную аутентификацию, единую точку входа (Single Sign-On), управление пользователями и их правами, а также защиту от кибератак и утечек данных. Платформа предоставляет гибкие возможности настройки, что позволяет адаптировать решения под конкретные нужды бизнеса и повысить уровень безопасности и удобства для конечных пользователей." data-html="true" data-original-title="Customer Identity Cloud" >Customer Identity Cloud (CIC). Атаки направлены в первую очередь на уязвимость в аутентификации между разными источниками (Технология Cross-Origin Authentication (аутентификация между источниками) позволяет пользователям проходить процесс аутентификации на одном домене, а затем использовать полученные учетные данные для доступа к ресурсам на другом домене. Это упрощает взаимодействие между разными веб-приложениями и сервисами, предоставляя единый вход для пользователей. Однако такая технология требует повышенного внимания к безопасности, чтобы предотвратить атаки, связанные с подстановкой учетных данных и другими киберугрозами." data-html="true" data-original-title="Cross-Origin Authentication" >Cross-Origin Authentication).

Подозрительная активность началась 15 апреля 2024 года. Okta оперативно уведомила клиентов, у которых эта функция была включена, но не раскрыла точное количество пострадавших.

Подстановка учётных данных — это тип кибератаки, при котором злоумышленники пытаются войти в онлайн-сервисы, используя уже доступный список имён

пользователей и паролей, полученный из предыдущих утечек данных, фишинговых атак или вредоносного ПО.

Okta рекомендует пользователям проверить журналы на наличие неожиданных событий входа, таких как неудачные попытки аутентификации между разными источниками (failed cross-origin authentication, fcoa), успешные попытки такой аутентификации (success cross-origin authentication, scoa) и утечки паролей (password leak, pwd_leak). Также компания советует сменить учётные данные и ограничить или отключить аутентификацию между разными источниками.

Клиенты компании, вероятно, были подвергнуты атаке методом подстановки учётных данных, независимо от использования данного типа аутентификации, если в журналах событий присутствуют scoa или fcoa и наблюдается рост неудачных попыток входа.

Среди других мер по смягчению последствий атак — включение обнаружения утечек паролей или Credential Guard, запрет на использование слабых паролей и внедрение методов аутентификации без паролей, устойчивых к фишингу, с использованием новых стандартов, таких как технология Passkey — это метод аутентификации, который позволяет пользователям входить в систему без использования традиционных паролей. Вместо этого используется криптография с открытым ключом, где приватный ключ безопасно хранится на устройстве пользователя, а публичный ключ — на сервере. Этот механизм обеспечивает улучшенную безопасность, устойчивую к фишингу, и упрощает процесс аутентификации." data-html="true" data-original-title="Passkey" >Passkey.

Ранее Okta уже предупреждала о росте частоты и масштабов атак методом подстановки учётных данных на онлайн-сервисы, которые поддерживаются с помощью локальных прокси-сервисов.